NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

Serial: N/0582
26 April 1983

MEMORANDUM FOR THE EXECUTIVE SECRETARY, IG/CM

SUBJECT: Proposed New Agenda Item

1. Enclosed for consideration as an IG/CM agenda item is an issue paper on cryptographic access requirements and an associated proposed NSDD entitled "Safeguarding Cryptographic Information and Material."

2. The National Security Agency believes a formal cryptographic access program is the key element in our efforts to counter the HUMINT threat to U.S. cryptography. Pursuing the initiative begun in NSDD-84, our proposed NSDD would establish a national cryptographic access program based on several criteria, including a requirement for consent to aperiodic, limited polygraph examinations.

3. I recommend the enclosure be circulated to the members for discussion at our next meeting.

HAROLD E. DANIELS, JR.
NSA Representative, IG/CM

Encl:
a/s

NSA review completed

Attach. 4

Issue Paper

Cryptographic Access Requirements

1. Prior to August 1973, a formal cryptographic access program was a national requirement. In addition to restricting access to classified cryptographic information to U.S. citizens with appropriate clearance and the need-to-know, the program required: (a) formal indoctrination stressing the unique nature of cryptographic information, its criticality, the special security regulations governing its handling and protection, and the penalties prescribed for its willful disclosure; and (b) formal records of all individuals granted cryptographic access.

2. In August 1973, the requirements for the formal indoctrination and recordkeeping were discontinued, effectively ending the formal cryptographic access program. This was done primarily to eliminate the administrative burden for military users of codes and secure voice equipments in Vietnam. In the succeeding decade, there has been a steady increase in insecurities involving cryptographic information and materials. The increased incidence of insecurities is damaging to the national security. Although it is attributable in some measure to the proliferation of cryptographic information and materials, the nature of the insecurities indicates a more serious cause, a lack of appreciation for protecting cryptography. This, in turn, is linked to the lack of a formal indoctrination requirement. Furthermore, the lack of formal records hampers the conduct of studies and investigations of insecurities and unauthorized disclosures. Additionally, the lack of signed access statements weakens prosecution in espionage cases.

3. While the foregoing are serious concerns, the greatest concern which the proposed cryptographic access program is directed toward is the HUMINT threat from cognizant agents. The key element of this program is the aperiodic, limited polygraph examination. We believe it is the most effective measure for detecting properly cleared individuals who have given or sold classified cryptographic information to unauthorized individuals. There are sufficient cases on record to give cause for grave concern. An equally important aspect of the aperiodic, limited polygraph examinations is their value in deterring individuals who have access and who might otherwise be inclined to give or sell classified cryptographic information to unauthorized individuals.

4. There is ample justification for reinstituting the proposed cryptographic access program with the added requirement for consent to aperiodic, limited polygraph examinations. The proposed NSDD (attached) is considered an appropriate means of accomplishing this, particularly in view of the recently issued NSDD-84, "Safeguarding National Security Information," which also addresses the use of the polygraph to safeguard classified national security information.

Encl:
a/s

Approved For Release 2007/11/01 : CIA-RDP96B01172R000600020016-8

Proposed National Security Decision Directive

Safeguarding Cryptographic Information and Material

Cryptography is especially sensitive because it is used to protect highly classified and critical information on almost every conceivable subject related to the operations and plans of the U.S. Government. For this reason, cryptographic information and materials are highly prized targets of hostile intelligence activities and must be strictly safeguarded. Access to cryptography, therefore, must be restricted to the greatest extent practicable and be consistent with national security needs. Accordingly, I direct that a cryptographic access program be established within each Federal department and agency which holds or uses cryptographic information or materials, consistent with the following:

a. Access to information which reveals the design of a classified cryptographic logic, its theory of operation, or access to classified cryptographic keying variables designated "CRYPTO" may be granted only when:

(1) The need for such access is established as necessary to perform official duties by, for, or on behalf of the U.S. Government.

(2) The individual requiring such access is a U.S. citizen, a non-U.S. citizen member of the U.S. military services, or a non-U.S. citizen employee of the U.S. Government.

(3) The U.S. Government has granted the individual a final security clearance.

(4) The individual has completed an indoctrination covering: 1) the sensitivity of cryptographic information and materials; 2) the rules for safeguarding such information and materials; 3) the rules pertaining to foreign contacts, visits, and travel; 4) the rules and procedures for reporting insecurities of COMSEC materials; and 5) the laws pertaining to espionage.

(5) The individual has executed a security agreement. All such agreements shall, at a minimum, provide for:

(a) Prepublication review to ensure deletion of classified cryptographic and any other classified information from information or materials to be disclosed.

(b) The individual's consent to participate in aperiodic, limited polygraph examinations consisting solely of questions related to disloyal activities and espionage when so required.

(c) The individual's acknowledgment of the sensitivity of, and obligation to protect, cryptographic information and materials.

Enclosure

Approved For Release 2007/11/01 : CIA-RDP96B01172R000600020016-8

(d) The individual's acknowledgment of his/her obligations to comply with applicable regulations governing unofficial foreign travel and contact with representatives of foreign governments.

All such agreements shall be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States and consistent with the standards developed by the Director, Information Security Oversight Office (ISOO), to satisfy these requirements.

b. In support of the cryptographic access program, the heads of Federal departments and agencies are responsible for:

(1) Restricting access to classified cryptographic information and classified cryptographic keying variables designated "CRYPTO" only to those persons who have been formally granted cryptographic access for the conduct of official business.

(2) Formally granting cryptographic access only when all the criteria set forth herein are met and maintaining records of individuals granted cryptographic access.

(3) Developing programs for the aperiodic, limited polygraph examination of personnel granted access; administering the polygraph programs; and evaluating the results of polygraph examinations. Departments and agencies with substantial polygraphing resources are encouraged to extend these resources to other departments and agencies whose limited requirements do not justify the acquisition of separate polygraphing resources.

(4) Establishing a quality control review over their respective polygraph programs to ensure the propriety of polygraph examinations, consistent with paragraph a.(5), above, and to protect individuals' rights.

(5) Reporting to the FBI and other appropriate investigative agencies information which indicates possible espionage or other unlawful activities involving classified cryptographic information or materials. Promptly advising the Director, NSA, of such incidents; the Director, NSA, will provide technical assistance as needed in the investigation of such incidents.

(6) Incorporating into contracts, where necessary, and ensuring compliance with the special security requirements associated with access to cryptographic logic, cryptographic design information, theory of operation, or cryptographic keying variables designated "CRYPTO."

(7) Recognizing the cryptographic access authorizations granted to individuals by other departments and agencies.

c. The Secretary of Defense, as Executive Agent for Communications Security, is directed to promulgate or revise national communications security policies and directives, as necessary, to implement the cryptographic access program described herein. These policies and directives will be promulgated through the national communications security issuance system.

25X1 CCIS/ICS: [redacted]

Distribution of D/ICS-83-0676

1 - Gen. Stilwell, OSD
5 - Mr. Snider, OSD (to be distributed to Army, Navy, Air Force and Marine Corps)
1 - Mr. Du Hadway, FBI
25X1 1 - [redacted] CIA
1 - Mr. McDonald, State
1 - Mr. Daniels, NSA
1 - Mr. deGraffenreid, NSC
25X1 1 - [redacted] DIA (for JCS)
1 - Mr. Leidenheimer, SECOM
1 - Ms. Lawton, DOJ
1 - Mr. Cinquegrana, DOJ
1 - Mr. McBrien, Treasury
1 - Mr. Peterson, Commerce
1 - Mr. Wingfield, Energy
1 - ICS Registry
1 - CCIS subject
1 - C/CCIS chrono

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Seventh 16/CM Meeting Agenda

FROM	EXTENSION	NO.
[redacted] C/IPB/PPG/OS 4E-70, HQS		STAT
	DATE 12 Aug 83	STAT

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
[redacted]				
C/OS/ISB				
3.				
4. O-1: Tom - you are on				
5. distribution for the Countermeasures				
6. Study; Dgov [redacted] a				STAT
7. copy today. You might want to				
8. look at pp 307-1089 the Study.				STAT
9. I don't think any additional				
10. input is needed for the				
11. meeting on 22 August.				
12. This is just to let you know				STAT
13. how much fun you're				STAT
14. missing. Fred				
15.				

Attached is F41. Issues in sections I and II will be addressed and actions will be assigned. The Agency's position on most of these items was made clear in the Organizational Study. I will be preparing "bullets" for [redacted] on each item so that he can comment, if necessary, at the meeting. I heard from [redacted] today that he will be doing a write-up on Resource Management for CM Programs, come 1 Oct 83. Fred

FORM 1-79 610 USE PREVIOUS EDITIONS